CYBER TOPICS, ANNOTATED

CSC MCU AY 2014-2015

M. Flynn, Professor of War Studies, CSC, MCU

CSC attendees are examining a number of issues to help increase conceptual understanding of cyber related to C2, manpower, and doctrine.

The cultural parameters helping to define leadership in cyberspace shapes the generational study of Josh Mayoral's, "World's Apart: US Decision Makers and the Generation Gap in Cyberspace."

Population shifts generating national security concerns become the focus of two studies looking at the impact of the megacity on cyber, and vice versa, in Joe Farina's, "Cyberspace in the Megacity: Thickening the Fog of War?," and Colin Relihan's (DIA), "Ending Virtual Resistance Networks in the Megacity." Their analysis reflects the Advanced Studies Program's cyber dimension.

How cyber impacts command and control is evaluated in three studies: John Hooks', "Command and Control in Korea: Satellite Communications in a Degraded Cyber Environment," Atiim Phillips', "USCYBERCOM's Lack of COCOM Authority: Examining C2 Structure within the DODIN," Kevin Yost's, "Cyber and the C2 Crisis: Increasing Vulnerabilities in Modern Warfare."

Cyber as a standalone conflict is debated in analysis offered by Joe Farina's forthcoming article submission suggesting Russia's effort to do just this, "The Russo-Georgian War of 2008 as a Standalone Cyber Conflict," and a master's paper discrediting the idea of war only in the cyber domain, a conceit of past air theorists, as presented by Jennifer Kukla in, "Cyber and the Myth of the Bloodless Battlefield: The Cyber Domain Supporting a Combined Arms Fight."

Cyber and its possible ability to change longstanding policy frameworks is considered in Brian Quinn's, "Great Power Conflict in the Cyber Age: Cyber Diplomacy and Averting the Thucydides Trap," and Steven Skipper's, "Cyber Threats and DIME: Past, Present, and Future."

Paul Keener's work examining manpower issues in terms of WO training, "Professionalizing the Cyber Force: Changing the Restricted Officer Training Paradigm," asks the DOD to look within itself to generate more capable personnel who can conduct better network security.

Completion dates are early May. Students would welcome the chance to discuss the ongoing work with MARFORCYBER.

M. Flynn

War Studies, Command and Staff
Marine Corps University

Bibliography

Farina, Joseph I., Maj, USMC. "Cyberspace in the Megacity: Thickening the Fog of War?" Master's Paper, Command and Staff College, Marine Corps University, 2015.

Analyzes cyber's organic electromagnetic energy and corresponding information sharing devices in the megacity in order to increase a maneuver commander's situational awareness and overload an adversary's cognitive load through misinformation.

----------. "The Russo-Georgian War of 2008 as a Standalone Cyber Conflict." Article Submission, Forthcoming, 2015.

Argues that Russian efforts in this confrontation looked to establish cyber supremacy as its main goal, not as a means of preparing the battlefield for a conventional fight; it therefore serves as an example of future war as a standalone cyber conflict, something currently unfolding in this domain.

Hooks, John A., Jr., Maj, USMC. "Command and Control in Korea: Satellite Communications in a Degraded Cyber Environment." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Establishes how cyber realities are creating new C2 challenges in Korea that can potentially destabilize the peninsula by ironically, solving those very issues.

Keener, Paul, Maj., USMC. "Professionalizing the Cyber Force: Changing the Restricted Officer Training Paradigm." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Discusses the current training of Restricted Officers within the Marine Corps, specifically the 06xx community, and proposes a change in training based in part on the US Army's WO program and best practices within industry for cyber professionals.

Kukla, Jennifer A., Maj., USMC. "Cyber and the Myth of the Bloodless Battlefield: The Cyber Domain Supporting a Combined Arms Fight." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Questions the views of theorists arguing that the cyber domain will host conflict as a standalone reality, stressing the folly of this past line of reasoning in the air domain; instead, it stresses the need to incorporate cyber into a combined arms fight.

Mayoral, Joshua, Maj., USMC. "World's Apart: US Decision Makers and the Generation Gap in Cyberspace." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Asks if cyber leaders in the US military, who missed the rapid technological evolutionary steps from 1979 to the present, lack a critical understanding that would give them a clearer vision of cyber operations and strategy.

Phillips, Atiim, Maj., USMC. "USCYBERCOM's Lack of COCOM Authority: Examining C2 Structure within the DODIN." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Examines the need to elevate USCYBERCOM to a full unified combatant command with specialized COCOM authorities given necessary changes to the DODIN C2 framework.

Quinn, Brian, Lt Col., USAF. "Great Power Conflict in the Cyber Age: Cyber Diplomacy and Averting the Thucydides Trap." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Advocates for diplomatic efforts between the United States and China to set the norms and standards of cyberspace for the international community to prevent an escalating crisis from excessive risk-taking in the cyber domain.

Relihan, Colin, DIA. "Ending Virtual Resistance Networks in the Megacity." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Examines how a U.S. joint interagency task force can promote and secure local civilian social media networks to then provide an intelligence and information operations advantage against a non-state armed group.

Skipper, Steven, Maj., USAF. "Cyber Threats and DIME: Past, Present, and Future." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Evaluates the impact of those seeking to leverage the Internet to conduct nefarious network operations, thereby impacting the DIME construct and the whole of government approach to US national security efforts.

Yost, Kevin, LCDR, USN. "Cyber and the C2 Crisis: Increasing Vulnerabilities in Modern Warfare." Master's Paper, Command and Staff College, Marine Corps University, 2015.

Reveals command and control as a critical vulnerability given the U.S. military's current dependence on the cyber domain that is notorious for its lack of information assurance; the age of modern warfare has created more vulnerabilities than advancements in technology have solved.